UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/771,840	02/04/2004	Art Shelest	MSFT121932	9753

26389 7590 07/26/2007

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/771,840	SHELEST ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-59 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-59 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see enclosed*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-59 are pending.

Information Disclosure Statement

2. The IDS submitted on 6/10/04 has been considered. An initiated copy is enclosed.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-47, 51, 52 and 57-59 are rejected under 35 USC 102(e) as being anticipated by Sobel et al. US Patent Application Publication No. 20040103310 (hereinafter Sobel).

5. As per claims 1-14, Sobel discloses a method for providing security in a computer system, comprising:

a. selecting a set of properties for use in determining members of a clean group (paragraph 20);

b. evaluating an item to determine if it has the specified set of properties, and if the item does have the specified set of properties, designating it as a member of the clean group (paragraph 21);

c. wherein the items are computers (paragraph 13);

d. wherein when a computer is to be evaluated, a clean component is installed on the computer to perform compliance checks (paragraph 19);

e. wherein a compliance check is performed at a selected time for an item to determine if the item has the specified set of properties (paragraph 20 and 24);

f. wherein one of the specified set of properties is whether all of the available updates have been installed (paragraph 17);

g. wherein the updates comprise at least one of security updates or service packs (paragraph 17);

h. wherein if the compliance check fails, a message is sent to indicate that the object should not be in the clean group; (paragraphs 21 and 24)

i. wherein if the compliance check fails, the clean group membership of the item is invalidated (paragraphs 21 and 24-27);

j. wherein the invalidation of the clean group membership comprises local actions which may include at least one of hiding or erasing the domain credentials of the item (optional);

k. wherein if the compliance check fails, additional steps may be taken including at least one of hiding cryptographic keys or logging out a privileged user (optional);

l. wherein if a compliance check passes, a message is sent to provide information that will be evaluated to determine if the item should be in the clean group (paragraphs 25 and 26);

m. wherein after a message is received and a determination is made that the item should be in the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group (paragraph 25; a timeout feature is inherent in connection oriented communications);

n. wherein an item in the clean group performs a self check to determine if it still has the specified set of properties, and if it does not, takes action to have itself removed from the clean group; (paragraph 24);

o. further comprising a clean group server, the clean group server initiating a status check to determine if the members in the clean group still have the specified properties (paragraph 20);

6. As per claims 15-25, Sobel discloses a system for managing security, comprising:

p. an update component which includes updates for items; a clean runtime component, the clean runtime component being installed on an item and being

able to communicate with the update component, the item becoming a member of a clean group when selected criteria are met; and a clean group server;

q. further comprising a domain controller which communicates with the clean group server; (fig. 1, reference nos. 110, 115, 120, 125, 130, 135)

r. wherein the items comprise computers (paragraph 13);

s. wherein compliance checks are performed for the items to determine if the items meet the selected criteria; (paragraph 20)

t. wherein one of the criteria is whether selected available updates have been installed; (paragraph 17)

u. wherein the updates comprise at least one of security updates or service packs; (paragraph 17)

v. wherein if a compliance check fails, a message is sent from the clean runtime component to the clean group server to indicate that the item should not be in the clean group; (paragraphs 21 and 24)

w. wherein if the compliance check passes, a message is sent from the clean runtime component to the clean group server to provide information that will be used to evaluate whether the item should be in the clean group; (paragraphs 25 and 26)

x. wherein after a message is received to indicate that the item should be placed in the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group;

(paragraph 25; a timeout feature is inherent in connection oriented communications)

y. wherein the clean runtime component performs a self-check of the item to determine if it meets the selected criteria for remaining in the clean group; (paragraph 24)

z. wherein the clean group server initiates a compliance check for items to determine if they should remain in the clean group. (paragraph 20)

7. As per claims 26-32, Sobel discloses one or more computer-readable media for providing security in a computer system, comprising:

aa. a runtime object which is installed on a computer, the runtime object being run on the computer to determine if the computer is in compliance, and based on the results of the compliance check sends a message regarding whether the computer should be in a group; (paragraphs 19-21)

bb. wherein the compliance check is performed initially upon installation of the runtime object; (paragraph 19)

cc. wherein the compliance check comprises a determination of whether selected available updates have been installed on the computer; (paragraph 17)

dd. wherein the selected available updates comprise at least one of security updates or service packs; (paragraph 17)

ee. wherein after a message is received to indicate that the computer should be placed in the group, a countdown is started and if another message is not

received by the end of the countdown, the item is removed from the group; (paragraph 25; a timeout feature is inherent in connection oriented communications)

ff. wherein the clean runtime object performs a compliance check on the computer (paragraph 20);

gg. wherein a group server communicates with the runtime object to initiate a compliance check (paragraphs 19 and 20).

8. As per claims 33-38, Sobel discloses a method for providing security in a computer system, comprising:

hh. determining if a computer is in compliance; and based on whether or not the computer is in compliance, disabling or enabling the computer domain account; (Abstract; paragraph 12)

ii. wherein when a new computer is to be added to the domain account, the new computer's account is placed in a disabled state until the computer is proved to be in compliance; (paragraphs 20, 21, 24 and 25)

jj. wherein when a new computer is to be added to the domain account, the domain join operation is predicated on proving that the computer is in compliance by requiring a clean group server to participate in the domain join operations; (paragraph 21)

kk. wherein the compliance check comprises determining whether available updates have been installed on the computer (paragraph 14);

ll. wherein the computer periodically performs compliance checks; (paragraphs 20 and 24)

mm. wherein a clean group server periodically initiates a compliance check on the computer (paragraphs 20 and 24).

9. As per claims 39-47, 51 and 52, Sobel discloses a method for providing security in a computer system, comprising:

nn. performing compliance checks for items; placing items which pass the compliance check into a clean group; and removing items from the clean group which fail the compliance check; (Abstract; paragraph 12)

oo. wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group; (paragraph 25; a timeout feature is inherent in connection oriented communications)

pp. wherein the item is a computer; (paragraph 13)

qq. wherein the item performs a compliance check; (paragraphs 20 and 24)

rr. wherein a clean group server initiates a compliance check on the item; (paragraphs 20 and 24)

ss. wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item; (paragraphs 14 and 17)

tt. wherein the item communicates with a clean group server to establish its membership in the clean group; wherein the clean group server communicates with a domain controller; (fig. 1, reference nos. 110, 115, 120, 125, 130, 135)

uu. wherein a compliance check may be initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy; (fig. 3)

vv. wherein an item may be a user, and a user's clean group membership is evaluated on the basis of whether the user's computer is in compliance; (paragraph 12)

ww. wherein a clean group is utilized to implement a computer security policy. (paragraph 17)

10. As per claims 57-59, Sobel discloses a method for providing security in a computer system, comprising:

xx. performing a compliance check for an item; and based on the results of the compliance check determining whether the item should be in a group; (paragraph 12)

yy. wherein if the item passes the compliance check, it is placed in a clean group (fig. 3, reference no. 335);

zz. wherein if the item fails the compliance check, it is placed in a dirty group. (fig. 3, reference no. 345)

11. Claims 39, 41-49. 51 and 52 are rejected under 35 U.S.C. 102(e) as being anticipated by Herrmann et al. US Patent Application 20040107360 (hereinafter Herrmann).

12. As per claims 39, 41-49, 51, 52 Herrmann discloses a method for providing security in a computer system, comprising:

aaa. performing compliance checks for items; placing items which pass the compliance check into a clean group; and removing items from the clean group which fail the compliance check; (paragraph 96)

bbb. wherein the item is a computer; (fig. 4, reference no. 310)

ccc. wherein the item performs a compliance check; (paragraph 94)

ddd. wherein a clean group server initiates a compliance check on the item; (paragraphs 93-95)

eee. wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item; (paragraphs 79 and 97)

fff. wherein the item communicates with a clean group server to establish its membership in the clean group; (paragraph 76-79 and 93-95)

ggg. wherein the clean group server communicates with a domain controller; (fig. 4, reference nos. 320, 330, 440, 450 and 460);

hhh. wherein a compliance check may be initiated by one or more of a client coming online, changes in client status/configuration, changes in network

status/configuration, or changes to a compliance policy; (fig. 7A, reference no. 701)

iii. wherein a clean group server communicates to non-compliant items how to get back into compliance; (paragraph 79 and 97)

jjj. wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated; (paragraph 79 and 97)

kkk. wherein an item may be a user, and a user's clean group membership is evaluated on the basis of whether the user's computer is in compliance; (fig. 4, reference no. 310 and related text)

lll. wherein a clean group is utilized to implement a computer security policy; (paragraphs 76-79)

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sobel in view of Lineman et al. US Patent Application Publication No. 20030065942 (hereinafter Lineman).

15. As per claims 53-55, the rejection of claim 52 under 35 USC 102(e) as being anticipated by Sobel is incorporated herein. Further, Sobel discloses the security policy provides communication requirements and parameters (paragraph 17). Sobel does not disclose wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. Lineman discloses a method and apparatus for managing security policies, including a common feature to provide limited access to published security policies that include the following steps: preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Sobel to enforce the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one

another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. One would be motivated to do so to significantly enhance the communication of these security policies to the users. Lineman, ibid.

16. Finally, Sobel does not disclose the security policy provides IPSec communication requirements and parameters. However, it is notoriously well known in the art that IPSec communications provides secure communications between a sender and a receiver to ensure that communications are not monitored by an unscrupulous 3rd party. In addition, IPSec protocols operate in the network layer to provider greater flexibility over other secure protocols such as SSL. Examiner takes Official notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the security policy to provide IPSec communication requirements and parameters. One would be motivated to do so to provide flexible and secure communication between a sender and a receiver. The aforementioned cover the limitations of claims 53-55.

17. As per claim 56, the rejection of claim 55 under 35 USC 103(a) as being unpatentable over Sobel in view of Lineman is incorporated herein. Sobel does not expressly disclose wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. However, it is notoriously well known in the art at the time of invention to invalidate policy settings when a client is no longer part of a group. For example, users

access means, such as passwords and usernames are conventionally deactivated or deleted by an administrator when a user is removed as a client. Examiner takes Official notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Sobel to include the step of wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. One would be motivated to do so to prevent access by a user whose privileges have been revoked as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 56.

18. Claims 50 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herrmann in view of Lineman et al. US Patent Application Publication No. 20030065942 (hereinafter Lineman).

19. As per claim 50, the rejection of claim 48 under 35 USC 102(e) as being anticipated by Herrmann is incorporated herein. Herrmann does not disclose wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. However, automation of a step is deemed to be an obvious enhancement. In re Venner, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958). It would be obvious to one of ordinary skill in the art at the time of invention to modify the invention of Herrmann to include the feature wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a

user's involvement. One would be motivated to do so to replace the manual activity with an automatic means of making the non-compliant item to be compliant as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 50.

20. As per claims 53-55, the rejection of claim 52 under 35 USC 102(e) as being anticipated by Herrmann is incorporated herein. Further, Herrmann discloses the security policy provides communication requirements and parameters. Herrmann does not disclose wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. Lineman discloses a method and apparatus for managing security policies, including a common feature to provide limited access to published security policies that include the following steps: preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the

invention of Herrmann to enforce the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. One would be motivated to do so to significantly enhance the communication of these security policies to the users. Lineman, ibid.

21. Finally, Herrmann does not disclose the security policy provides IPSec communication requirements and parameters. However, it is notoriously well known in the art that IPSec communications provides secure communications between a sender and a receiver to ensure that communications are not monitored by an unscrupulous 3rd party. In addition, IPSec protocols operate in the network layer to provider greater flexibility over other secure protocols such as SSL. Examiner takes Official notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the security policy to provide IPSec communication requirements and parameters. One would be motivated to do so to provide flexible and secure communication between a sender and a receiver. The aforementioned cover the limitations of claims 53-55.

22. As per claim 56, the rejection of claim 55 under 35 USC 103(a) as being unpatentable over Herrmann in view of Lineman is incorporated herein. Herrmann does

not expressly disclose wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. However, it is notoriously well known in the art at the time the invention was made to invalidate policy settings when a client is no longer part of a group. For example, users access means, such as passwords and usernames are conventionally deactivated or deleted by an administrator when a user is removed as a client. Examiner takes Official notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Herrmann to include the step of wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. One would be motivated to do so to prevent access by a user whose privileges have been revoked. The aforementioned cover the limitations of claim 56.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See enclosed PTO-892.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung Kim
Examiner
AU 2132
July 18, 2007